*MEDDAC MEMO 380-3

DEPARTMENT OF THE ARMY
U.S. ARMY MEDICAL DEPARTMENT ACTIVITY
FORT HUACHUCA, ARIZONA 85613-7040

MEDDAC MEMORANDUM 18 February 2005
No. 380-3

Security

MEDDAC/DENTAC SECURITY PROGRAM

1. HISTORY. This issue publishes a revision of this publication.

2. PURPOSE. This policy establishes security measures for the protection of USA MEDDAC personnel, patients, visitors, equipment, and facilities. This memorandum is designed to protect and safeguard all assets from sabotage, terrorism, theft, malicious damage, and dishonest, illegal or criminal acts. Security issues will be address by investigations, inspections, spot checks, interviews, and by conducting training.

---

* This memorandum supersedes MEDDAC Memo 380-3, 15Feb01

3. SCOPE. This policy applies to all units and activities assigned or occupying facilities of USA MEDDAC.

4. REFERENCES.

4.1 AR 190-13, The Army Physical Security Program.

4.2 AR 190-40, Serious Incident Report

4.3 AR 190-51, Security of Unclassified Army property (sensitive and non-sensitive).

4.4 AR 380-5, DA Information Security Program

4.5 FH Reg 190-1, Intrusion Detection System

4.6 MEDCOM Pamphlet 190-2, Handbook for U.S. Army Medical Command security Officers.

4.7 MEDCOM Pamphlet 190-31, A Guide for Crime Prevention Officers.

4.8 MEDCOM Supplement 1, AR 190-13, The Army Physical Security Program.

5. RESPONSIBILITIES.

5.1 The Commander is responsible for establishing physical security standards, designating Mission Essential/Vulnerable areas, and supporting this publication.

5.2 Designates an individual responsible for establishing, implementing, and monitoring a security program. Acts as the administrative proponent for the annual review and update of established policies and procedures. Furnishes guidance and interpretations of references for department chiefs. Responsible for:

5.2.1 Establishing, interpreting, and implementing security regulations, and directives.

5.2.2. Conducting semi-annual physical security inspections and monthly crime prevention checks.

5.2.3 Coordinating security training for military and civilian personnel.

5.2.4. Providing technical advice and assistance to individual sections concerning the establishment and implementation of internal security policies.

5.2.5 Designates someone to serve as an active member of the Safety Committee and report security issues that pertain to safety during the Safety Meetings.

5.2.6 Liaison between the installation Force Protection Agency, Military Polices, civilian authorities and USA MEDDAC.

5.2.7 Conduct an annual evaluation and self-assessment of the physical security program (PSP).

5.3 Department chiefs are responsible for ensuring that individual sections under their control comply with this publication. Department chiefs will review the PSP annually and furnish their goals and objectives for enhancing security. Responsible for supporting MEDDAC's PSP.

5.4 The Fort Huachuca Military Police(MP) are responsible for supporting the MEDDAC on law enforcement issues. The MPs respond to audio and telephonic request for assistance on criminal acts, traffic control during medical emergencies, natural disasters, or man made disasters.

The proponent of this publication is the Chief, Mobilization, Education, Training and Security Division. Users are invited to send comments and suggested improvements on DA Form 2028 directly to MCXJ-METS, USA MEDDAC, Fort Huachuca, Arizona 85613-7040.

FOR THE COMMANDER:

OFFICIAL:

NOEL J. CARDENAS
MAJ, MS
Deputy Commander for
Administration

ROBERT D. LAKE
Information Management Officer

DISTRIBUTION: B

APPENDIX A
Threat Statement

1. Physical and procedural security measures are critical to the protection of MEDDAC assets. Although established regulatory guidelines mandate the physical security measures applied to protect MEDDAC assets, the local threat indicators are continuously monitored and are instrumental in updating the physical security program as necessary.

2. General threat capabilities. Because of the open nature of MEDDAC facilities, there is a vulnerability to certain aggressor activities. Even if a specific threat has not been made against critical assets, security of these assets is a continuous concern. The following assessments were compiled from information obtained from the FT Huachuca Installation Threat Assessment and local law enforcement agencies.

a. Protesters: In the past, Fort Huachuca has been site of demonstrations, although none has escalated to violence. Still, each demonstration has inherent security issues such as access control and damage to government property. The assessed threat of demonstrations/protest is low.

b. Terrorists: There is no intelligence indicating that terrorist are targeting Fort Huachuca personnel or facilities. Despite this, the terrorist threat level remains difficult to accurately assess. It is extremely important that personnel remain vigilant and report all suspicious activity.

c. Vandals: At this time threats of vandalism are low. Even if local gang activities were to increase, it is not expected to pose any threat to MEDDAC and its activities.

d. Violence in the workplace: Violence in the workplace remains low. Workload demands on the civilian and military work force, commonly viewed as “do more with less” philosophy, it is quite capable of increasing employee frustration, irritability, anger, failures to obey policies, and the feeling of being a victim. Coupled with changes in the work force through restructuring and deployment of soldiers are a cause for concern.

d. Insider Compromise: The greatest threat to MEDDAC is from insider compromise. Insiders commit criminal or terrorist acts, motivated by greed, which creates the most significant threat to MEDDAC assets and functions.

3. To prevent the compromise of assets by the range of aggressors discussed, it is necessary to provide an integrated physical security program. The Program must combine physical, personnel, telecommunication, and information security to effectively provide the fullest protection possible.

Appendix B
Patient and Visitor Control

1. Access to costly supplies and equipment by increasingly large numbers of patients and visitors make the clinics extremely lucrative targets for theft. For this reason, the security needs of our facilities exceed those of virtually any other activity on the installation.

2. Access control effectively discourages criminal activity and is very much a part of the security system. The following procedures are established to control access in the Health Center without denying or delaying treatment to authorized personnel:

a. Idle, curious, or suspicious person should not be allowed to wander about at will. Offer to assist or escort those who appear to be lost or in need of help.

b. Continuously challenge unknown or suspicious persons. Question those who claim to be visitors. Their response may give them away if they are unable to name the person or clinic they are visiting.

c. Report encounters or suspicions to the security office, 533-2491/5179. Allow law enforcement to confront those personnel who may pose a physical threat.

d. Encourage the use of designated clinic waiting areas. Such areas are convenient, yet tend to limit or restrict patient and visitor movement thereby reducing opportunities for criminal behavior.

e. Not all personnel who pass through the doors are entitled to medical treatment. Some see the clinics as possible targets for theft or other criminal behavior. Discourage those who mean harm, stay alert, enforce staff/patient controls, and report suspicious behavior either to the Security Office 533-2491/5179 or AOD 533-2963.

Appendix C
Identification Badge Assignment

1. All personnel assigned or attached to USA MEDDAC, to include volunteers and contractors, are required to wear a pictured identification badge. Badges will be displayed on the outside of all garments and upper torso for easy identification. Badges will not be worn at the waist. For active duty the badge will be worn on the left upper pocket of the BDU.

2. Personnel will report to the security office to receive a badge assignment. Individuals will surrender their badge to METS in the event of ETS, PCS, retirement, or termination.

a. Official Visitors; Official visitors are required to wear a visitor’s badge for the duration of their stay.

b. Contract workers: All contract workers will wear a visitor’s badge. The Division responsible for the contract workers will ensure the badges are issued and returned upon departure of the contract workers.

c. Volunteers: All volunteers will display a badge signifying their status as a volunteer.

3. Lost and found badges will immediately be reported/turned into the Security office.

4. Point of contact is the Security Manager at 353-2491/5179.

Appendix D
Mission Essential/Vulnerable Areas (MEVA)

Mission essential/vulnerable areas are designated by the commander IAW AR 190-13 and MEDCOM PAM 190-2. These areas are critical to sustain the operation of the facility and are vulnerable to theft, trespass, damage or other criminal acts. These areas and standards of protection are:

Area	Standards
Medical Service Accounts	2,5,6
Pharmacies	1,3,4,5,6,7
Controlled Substance Vault	1,3,4,56,
Medical Supply Warehouse	2,4,5,6
Generator	2,4,5,6
Patient Record Storage Area	2,5,6,
CHCS Control Point	2,6,7
Classified Document Storage Area	2,4,5,6
Computer Control Center	1,5,6
Surgical Suite	2,5,6,

SECURITY STANDARDS:

1-Controlled Access Area
2-Limited Access Area
3-Requires Intrusion Detection System
4-Requires permanently affixed window or bars
5-Requires key and lock control system
6-Requires interior and exterior security lighting
7-Requires storage in a vault
8-Requires storage in a safe
9-Requires fenced enclosure

Appendix E
Intrusion Detection Systems

1. Intrusion Detection Systems (IDS) are used to enhance security for areas that contain items of great interest or value.

2. All IDS (including motion sensors) will be tested on a quarterly basis. The NCOIC is responsible for conducting these tests and maintaining verification documentation. Procedures for conducting the quarterly alarm test are as follows:

a. The NCOIC will make necessary arrangements with the MPs and or appropriate agency to schedule dates and times for testing of the alarms.

b. Test results will be annotated on the DA Form 4930-R, forwarded to and maintained by the Security Manager.

c. If an alarm is found deficient, the NCOIC will coordinate repair requests with Security Manager.

3. Operation procedures. During non-duty hours, the alarm systems are monitored by the Military Police.

Appendix F
Building, Office and Equipment Security

1. Primary responsibility for building/office security rest with the Unit Commander or the Activity Chief whose operations encompass the use of the area. The last individual to depart their area will ensure that:

a. All safes are secured, if applicable.

b. All windows and doors are secured.

c. All electrical appliances are turned off if applicable.

d. All filing cabinets are locked if containing sensitive information.

e. All unused sharps are secured.

f. Ensure prescription pads, medical records, or any other sensitive items are secured.

g. No fire hazards exists.

h. After verifying all the above, the individual will annotate findings on Standard Form 701.

2. The hand receipt holder for each area is responsible for securing office equipment (i.e, computers systems, TVs, etc).

Appendix G
Traffic Control

1. Fire lanes and handicap parking spaces have been identified by signs. Violators will be reported to the Military Police at 533-2181.

2. Operations during medical emergencies. The Security Manager will coordinate with the Military Police for traffic control. MEDDAC personnel selected from the manpower pool will be utilized as a guard force for assisting the Military Police in traffic control.

Appendix H
Child Security Plan

1. Preventive measures have been implemented through out the facility in efforts to minimize the chance of an infant/child being abducted.

2. The abductor will be detained from exiting the facility/area whenever possible. To avoid possible injury to the child or staff, physical detention will not be used to prevent the abductor from leaving the area. When possible gather all available information(i.e, physical description of abductor, clothing, make and model of car, license plate number, direction of travel, and any other information that may be valuable to the military and civilian authorities). Information such as description of abductor and vehicle should be written down as soon as possible. USA MEDDAC personnel will assist the authorities.

3. Staff on duty when the abduction occurs will remain in their unit/section until the authorities have completed their questioning. Staff will refrain from discussing the incident with anyone other than authorities.

4. The Public Affairs Officer(PAO) will clarify and coordinate specific requests with media coverage and assistance with contacting other family members.

5. At no time should anyone without a valid need-to-know be told that a child is missing. Personnel are not authorized to make a public statement concerning this incident or to communicate with a member of the media without prior clearance from the PAO and Commander.

6. Search Concept: The entire facility will be searched with special emphasis applied to common areas (i.e. restrooms, closets, etc). Refer to the Emergency Management Plan.

APPENDIX I
Weapons in the Health Center

1. DEFINITION: Weapons are defined as any firearm, knife(straight, folding, or lock back with a blade length of 4 inches or greater), or any device designed to cause bodily harm or injury.

2. POLICY: Staff, visitors, or patients are strictly prohibited from carrying a weapon while in the Health Center. Only civilian and military law enforcement authorities on official business are authorized to carry an assigned weapon.

3. PROCEDURES:

a. During normal duty hours the Security Manager or the Military Police will be notified immediately of an individual known or suspected of carrying a weapon. The Security Manager will contact the proper law enforcement authorities and will safeguard any confiscated weapons until the arrival of the proper authorities. The AOD will assume the responsibilities of the Security Manager during non-duty hours.

b. If an individual becomes disruptive or argumentative when asked to surrender the weapon, contact the Military Police. Do not attempt to confront the individual.

c. Weapons, dangerous devices, contraband, or suspected stolen property will be retained for law enforcement authorities.

Appendix J
Investigating and Reporting Security Incidents

1. Procedures for investigating and reporting security incidents vary with the type of incident. An incident that requires immediate attention or that might concern the Department of the Army would be reported within a very stringent timeframe where most other incidents would follow channels. The Security Manager will investigate all security incidents upon notification and follow reporting procedures governed by this policy.

2. Once notified of a security violation/incident, the Security Manager will conduct an informal investigation. The investigation will consist of reporting to the vicinity of the incident, conduct a visual check of the area, and conduct verbal conversations(s) with witness(s)/victim(s). The Security Manager will report all findings to the Commander or his/her representative. If the situation cannot be resolved internally and the assistance of outside agency is required, the Security Manger is responsible for coordinating the formal investigation.

3. Non-serious incidents will be reported as follows:

a. The Military Police will be contacted telephonically 533-2181.

b. The Criminal Investigation Services will be notified by the Security Manager or Military Police for incidents requiring their services.

4. Incidents that are of a serious nature, actual or alleged, that warrants timely reporting to MEDCOM because of its nature, gravity, publicity, or potential consequences, will be reported using the Serious Incident Report reporting procedures kept in the security office.

Appendix K
Storage of Classified Material/Security Containers

1. Safeguarding classified information takes precedence over all other assigned tasks. The safe is located in METS and is utilized to store classified information.

2. Review the document to determine if the information contained warrants further dissemination. If so, ensure the individual with “need to know” has the level of clearance as high or higher than the document involved. Hand carry the document (with protective covering), to the appropriate area. Wait while the individual reviews the document. Once the individual has reviewed the document, return the document to the safe. Ensure the document is in your sight at all times.

3. Under no circumstances will classified information be reproduced using local reproduction machines.

4. File the document in the safe.

5. The security container in METS is designated as the “master container” and will store the combinations to all containers.

6. Combinations are changed annually, when the individual having access to the combination departs section, or whenever an individual who has knowledge of the combination no longer requires access. To change a combination, a memorandum must be forwarded to the security office with the following information:

   a. Location of safe (building number and room number).

   b. Serial number of safe.

   c. Point of Contact(POC).

7. Once the combination of the safe is changed, a Standard Form 700 will be completed by the POC and the combination to the safe will be stored in the master safe.

8. Unused security containers will have the combinations reset IAW AR 380-5.

9. OPEN/CLOSED signs are to be used on all active containers.

10. Use Standard Form 702, Security Container Check Sheet, for all active security containers and annotate each with the time the container was opened and closed. Check all security containers at the close of business, whether the container was opened or not opened that day. Personnel performing the checks may not be the same as the individual who locked the container, unless there is no one else available.

11. Keep the tops of all security containers free of extraneous material.

Appendix L

Physical Security Inspections

1. Formal inspections are conducted on a semi-annual basis for the pharmacy. Inspections are announced to prevent any interference with patient care. The inspections are conducted by MEDDAC Security Manager and by the post Force Protection Agency.

2. All sections of USA MEDDAC will be inspected annually by MEDDAC Security Manager to determine if physical security measures are adequate to provide protection from external and internal threat. Limited access areas and those areas designated as restricted are particularly important in this regard.

3. Some of the topics reviewed are;

a. Activity Security Checklist (SF 701): The checklist should be posted in a centralized location. This form is utilized to annotate daily checks ensuring areas are secured at close of business.

b. Controlled or Limited Access areas: These areas are checked to ensure access rosters are current, security levels are maintained, and staff are trained on emergency situations.

c. Security of sensitive items: Items such as needles, sharps, prescription pads, etc., are checked to ensure proper protection method are applied.

d. Cypher locks: Combination numbers will be changed annually or upon the departure of an individual from that work area.

e. Telecommunication Monitoring:

(1) Ensure signs are posted above all copiers and Facsimiles indicating “reproduction of classified information is prohibited”.

(2) Telephones receivers must display DD Form 2056. Also, a Bomb Threat checklist will be posted neat each telephone.

(3) Safes: Areas utilizing GSA approved safes will ensure a SF 702 (security container check sheet) is maintained. A SF 700 will be prepared and furnished to the security section, METS for safeguarding. The NCOIC will ensure the combination is changed IAW AR 380-5.

g. Key control; Review to verify that all key control policies are followed.

4. Once an inspection is completed the Physical Security Inspection Report is prepared. Distribution for this report is the NCOIC and Security for record. If a section fails two consecutive inspections, a formal report is submitted through the Deputy Commander of Administration to the Commander.

Appendix M

Physical Security Inspection Checklist

CHECKLIST	YES	NO
1. Are doors and windows throughout the facility in repair and do they provide good security?	___	___
2. Are all entrances equipped with secure locking devices? Are any doors propped opened?	___	___
3. Are all entrances always locked when not in use?	___	___
4. Are all windows securely fastened from the inside?	___	___
5. Are there adequate security lights being utilized?	___	___
6. Are all ventilators or other possible means of entrance to the facility covered with steel bars or adequate wire mesh?	___	___
7. Are only authorized padlocks being used IAW AR 190-51?	___	___
8. Has a key/lock custodian and an alternate key/ lock custodian been appointed?	___	___
9. Has a key box constructed of metal and securely fastened to the structure been installed?	___	___
10. Has a key control register been established to ensure accountability for all keys and is key access current.	___	___
11. Are 10% inventories of all keys assigned to essential personnel being conducted monthly, and are all keys being inventoried semi-annually?	___	___
12. Are key numbered IAW AR 190-51?	___	___
13. How many entrance/exit door keys does the facility have _____? Who maintains them? _____	___	___

14. Does the key custodian maintain a set of entrance keys. ___ ___

15. Are drugs, precious metals, needles, and syringes being stored in accordance with AR 190-51. ___ ___

16. Is the narcotic access current?

17. Do personnel know to report all security incidents to METS Division Security Manager ? ___ ___

18. Has the NCOIC gone over Bomb Threat Procedures and evacuating procedures? ___ ___

19. Do all personnel assigned understand and have access to the Bomb Threat Procedures? ___ ___

20. Are Bomb Threat cards placed under all active telephones in the facility/section/division, etc? ___ ___

21. Is there an evacuation plan current? ___ ___

22. Are all personnel trained on the evacuation plan? ___ ___

23. Are all personnel familiar with their assembly area? ___ ___

24. Is security training documented in personnel six sided folder? ___ ___

25. Do all personnel have and wear their MEDDAC Identification Badges? ___ ___

26. Is personal property secured? ___ ___

27. Is MEDDAC Memo 380-3 in security binder? ___ ___

28. Are cipher locks or safe lock combinations being changed at least once a year or whenever a person leaves that knew the combination? If not why? ___ ___

29. Are preferable supplies being stored in an area with limited access? ___ ___

30. Are end of day security checks being conducted? ___ ___

INSPECTION NOTES:

Appendix N
Key Control

1. A Key Control Officer will be appointed in writing. The individual will not be below the grade of 0-1 or GS-7. The Key Control Officer will oversee the organization's key control program and maintain key control regulation/policies. Additional duties of the Key control Office include:

a. Ensuring each area designates in writing a Key Control Custodian.

b. Ensuring assigned Key Control Custodians are trained in proper key control procedures.

c. Issuance of keys to area key custodians.

d. Overseeing semi-annual 100% key inventories.

e. Maintaining excess keys.

f. Ensuring proper key control procedures are being followed.

g. Determining legitimacy of request for additional keys.

h. Submit all request for key related issues to the Security Manager/Key Control Officer.

2. Key Custodians are appointed in writing. Responsibilities of the Key Custodians include:

a. Ensuring proper key control procedures are followed.

b. Reporting lost keys immediately to the Key Control Officer.

c. Ensuring all request of additional keys are justified.

d. Ensuring Alternate Key Custodians are trained in proper key control procedures.

3. The following standardizes key control procedures throughout the organization.

a. The Key Control Officer will issue keys to the Key Control Custodian for their appropriate area on a DA Form 5513-R.

b. Permanent retention keys are keys that will be maintained by the staff for the duration of their stay with a particular area. The Key Custodian will issue these keys to staff on a separate DA Form 5513-R

c. Non-retention keys are keys that are not issued on a permanent basis. Normally these keys are maintained in the key box until needed. If needed, these keys will be issued on a separate DA Form 5513-R on a temporary basis and will be returned to the key box prior to close of business.

d. The Key Custodians are responsible for conducting 10% monthly inventories of permanent retention keys. These inventories will be conducted on a show basis. Completion of these inventories will be annotated on the reverse side of the DA from 5513-R used to issue the keys.

e. Semi-annual inventories will be conducted on 100% of the keys issued by the Key Control officer. These inventories will be conducted by the Key control custodian. Completion of these inventories will be annotated on DA 5513-R.

f. Excess keys will be secured in a lockable key box or equivalent container constructed of at least 26 gauge steel. This container must be attached to the wall and access to this container will be limited to the key control custodians.

g. Lost or stolen keys will be reported in writing immediately to the Key Control Officer.

h. Request for additional keys will be submitted to the Key Control Officer in writing.

i. Alternate key custodians will not perform key control if the primary key custodian is available.

Appendix O
Civil Disturbances/VIPs/Media

1. If a civil disturbance occurs at a facility belonging to USA MEDDAC, the following steps will be followed:

a. Instruct staff not to get involved.

b. Immediately notify the Security Manager and the Military Police(MP).

2. Situations involving VIPs or the Media. During an emergency, VIPs and the Media will be directed to a designated area. The Public Affairs Officer will be available to deal with the situation.

3. Procedures dealing with traffic and human control near emergency areas will be as follows:

a. Traffic control: The Security Manager will contact the MPs to control traffic. Personnel from USA MEDDAC will assist the MPs.

b. Human control: The Security Manager or an authorized individual will select personnel from the manpower pool to perform guard duty. The guards will be positioned at areas near the emergency site. If necessary, the MPs will be contacted by the Security Manager for assistance.

4. Contingency Plan: In the event of an emergency situation resulting from civil disturbance, demonstrations, bomb threats, fires, disasters, etc., procedures and guidelines for handling such are in the MEDDAC’s Emergency Management Plan. This plan should be available in each department to be utilized if an emergency arises.

Appendix P
Security Orientation and Education Requirements

1. The Security Manager will establish and manage a Security Education Program utilizing applicable policies, procedures, and guidelines. Training is conducted as initial orientation and refresher.

a. Orientation Briefing: The purpose of this briefing is to provide newly arrived personnel an understanding of the local security policies. Briefing topics include policies such as bomb threat procedures, Operation Security (OPSEC) and Force Protection Standards.

b. Refresher Briefing: Refresher briefings are conducted during the Birth Month Annual Training sessions. Additional training is available on the Medical Education Personnel System or by contacting the Security manger for section training session.

2. Training for Sensitive Areas. Individuals working in sensitive areas are at greater risk due to information or items located in their respective areas. Annually training is conducted discussing the additional protective measures taken to protect equipment and personnel.